UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,483	11/17/2003	Simon Charles Watt	550-471	6434

23117 7590 11/02/2006

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
JOHNSON, BRIAN P	

ART UNIT	PAPER NUMBER
2183	

DATE MAILED: 11/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/714,483	WATT ET AL.	
	Examiner	Art Unit	
	Brian P. Johnson	2183	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 August 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

1. Claims 1-39 have been examined.

Acknowledgment of papers filed: amendments and remarks filed on 18 August 2006. The papers filed have been placed on record.

Specification

The title is accepted. Objection is withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8, 10-16, 18-36 and 38-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alverson's background (U.S. Patent No. 7,020,767) in view of Angelo (U.S. Patent No. 6,581,162).

Regarding claim 1, Averson discloses a system with multiple domains.

Alverson also discloses a protection requirement for the domains, but fails to disclose particular information about monitoring.

Angelo discloses a monitoring function within a processing system (col 7 line 40 to col 8 line 15).

Alverson, at the time of the invention, would have been motivated to use SMM and SMI in computer security memory management to protect against malicious

software and viruses, thereby improving computer security memory management. Furthermore, Alverson has shown an expressed desire for multiple levels of protection that is domain specific (col 2 line 56-57).

It would have been obvious at the time of the invention for one of ordinary skill in the art to take the system of Alverson and incorporate the SMM and SMI security of Angelo. The combination would be as follows:

Alverson/Angelo method of controlling a monitoring function of a processor (Angelo col 7 line 40 to col 8 lines 15), said processor being operable in at least two domains (col 1 lines 30-33), comprising a first domain and a second domain, said first and second domains each comprising at least one mode (col 7 line 61 to col 8 line 4), said method comprising the steps of: controllably monitoring (col 7 line 56-58) said processor operating in each of said at least two domains (col 1 lines 30-33 and col 2 lines 56-57—*Note that the citations indicate that Alverson desired a level of security that can vary in each domain*), setting at least one control value, said at least one control value (col 7 lines 56-58) relating to a condition and being indicative of whether said monitoring function is allowable in said first domain (col 7 line 61 to col 8 line 4); and only allowing initiation of said monitoring function in said first domain when said condition is present if its related control value indicates that said monitoring function is allowable; and not allowing initiation of said monitoring function in said first domain when said condition is present and its related control value indicates that said monitoring function is not allowable (col 7 line 61 to col 8 line 4).

Regarding claim 2, Alverson/Angelo discloses the method according to claim 1, wherein said first domain is a secure domain and said second domain is a non-secure domain (Angelo col 8 line 4), said processor being operable such that when executing a program in a secure mode within said secure domain said program has access to secure data which is not accessible when said processor is operating in a non-secure mode within said non-secure domain (Angelo col 8 line 11-15).

Note that a domain is considered to be in a secure mode when the SMI handler is running. At this point, it is a "secure domain". Otherwise, it is non-secure.

Regarding claim 3, Alverson/Angelo discloses the method according to claim 2, wherein said condition comprises a domain, mode or type of monitoring function (Angelo col 7 line 61 to col 8 line 4).

Regarding claim 4, Alverson/Angelo discloses the method according to claim 3, wherein said condition comprises a secure domain and said control value comprises a secure domain enable value, initiation of monitoring in said secure domain only being allowed if said secure domain enable value is set (Angelo col 7 line 61 to col 8 line 4).

Regarding claim 5, Alverson/Angelo discloses the method according to claim 3, wherein said secure domain includes a secure user mode and said condition comprises a secure user mode (Angelo col 8 line 1).

Note that the handler routine is considered to be the "secure user mode"

Regarding claim 6, Alverson/Angelo discloses the method according to claim 5 wherein said control value comprises a secure user mode enable bit (col 7 line 56-57) and initiation of monitoring from secure user mode is only allowed if said secure user mode enable bit has been set (Angelo col 7 line 61 to col 8 line 4).

Regarding claim 7, Alverson/Angelo discloses the method according to claim 4, wherein said condition comprises a type of monitoring function (Angelo col 8 line 1-4).

Regarding claim 8, Alverson/Angelo discloses the method according to claim 7, wherein said condition comprises a debug monitoring function and said control value comprises a debug enable bit, initiation of debug in said first domain only being allowable if said debug enable bit has been set (Angelo col 8 line 8-11).

Note that the monitoring function is considered to be a debug monitoring function.

Regarding claim 11, Alverson/Angelo discloses the method according to claim 1, said method comprising setting a plurality of control values, each of said plurality of control values relating to a different condition; and only allowing initiation of said monitoring function in said first domain if any of said conditions are present if each of said control

values related to a condition that is present indicate that said monitoring function is allowable (Angelo col 7 line 61 to col 8 line 11).

Note that the plurality of control values includes the SMI interrupt and the SMIACT signal.

Regarding claim 12, Alverson/Angelo discloses the method according to claim 1, said method further comprising said steps of: setting a control indicator, said control indicator indicating that monitoring is only allowable for specified applications; and prior to initialising said monitoring function checking an application identifier; and only allowing initiation of said monitoring function if said application currently running is one for which monitoring is allowable.

Note that Alverson/Angelo, as previously combined, does not necessarily disclose the limitations above. As originally combined, the SMI handler routine is domain specific; however, it would further be obvious to make these routines stream (or application) specific.

Alverson would have been motivated to utilize this technique since the invention is initially concerned with stream specific privileges (Alverson col 2 lines 56-57).

Regarding claim 13, Alverson/Angelo discloses the method according to claim 12, wherein the step of setting a control indicator comprises setting a control indicator stored in a predetermined position in a storage element.

Note that the use of a particular interrupt or signal suggests that it is held in a common register that is considered to be "a predetermined position in a storage element". More generally, in order for the signal to have the necessary effects, its position must be predetermined; otherwise, the processor would not know what the signal is attempting to signify.

Regarding claim 14, Alverson/Angelo discloses the method according to claim 12, wherein said monitoring function comprises monitoring said processor and capturing diagnostic data (Angelo col 7 line 64 to col 8 line 4), said method comprising the further step of: following initiation of said monitoring function only allowing capturing of diagnostic data in said first domain while an application running on said processor is one for which monitoring is allowable (see claim 12).

Regarding claim 15, Alverson/Angelo discloses the method according to claim 1, wherein said monitoring function comprises monitoring said processor and capturing diagnostic data (Angelo col 7 line 64 to col 8 line 4), said method comprising the further step of: following initiation of said monitoring function only allowing capturing of diagnostic data in said first domain when a condition changes if a control value related to the changed condition indicates that said monitoring function is allowable (Angelo col 8 line 8-11).

Regarding claim 16, Alverson/Angelo discloses the method according to claim 1,

wherein setting of at least one control value is performed either by setting said control value via an input port or by setting said control value from the first domain (Angelo col 7 line 56-58).

Regarding claim 17, Alverson/Angelo discloses the method according to claim 16, said method comprising the further step of blocking write access to said control value via said input port such that the step of setting said control value can henceforth only be performed by setting said control value from said first domain.

Note that the SMM signal, in some embodiments (Angelo see col 7 lines 56-58) does not require an input port. Consequently, these embodiments are considered to be blocked, leaving only modification from the first domain.

Regarding claim 18, Alverson/Angelo discloses the method according to claim 1, wherein said first domain comprises a first user mode (Alverson col 1 lines 30 to 33) and a first privileged mode (Alverson col 2 lines 56-57) and the step of setting at least one control value in said first domain (Angelo col 8 lines 8-11), comprises setting said control value from said first privileged mode.

Note that a level of privilege will often be activated (Alverson) when the SMI handler routine is called (Angelo)

Regarding claims 20-28, see claims 1-9,

Regarding claim 29, Alverson/Angelo discloses the processor according to claim 20, wherein: said storage element is operable to contain a plurality of control values, each of said plurality of control values relating to a different condition (Angelo col 7 lines 57-58 and col 8 lines 9-11); and said control logic is operable to only allow initiation of said monitoring logic in said first domain if any of said conditions are present if each of the control values related to a condition that is present indicate that the monitoring logic is allowable (Angelo col 7 lines 61-64).

Regarding claim 30, Alverson/Angelo discloses the processor according to claim 29 wherein one condition comprises a secure domain and a corresponding control value comprises a secure domain enable bit (Angelo col 7 line 61 to col 8 line 4) and a further condition comprises a secure user mode and a corresponding control value comprises a secure user mode enable bit (Alverson col 1 lines 30-33—*note that the secure user mode and secure mode of the domain are considered to be the same)*, said control logic being operable to initiate said monitoring logic from secure user mode only when said storage element contains both a secure user mode enable bit and a secure domain enable bit (Angelo col 7 line 61 to col 8 line 4).

Regarding claim 31, Alverson/Angelo discloses the processor according to claim 20, wherein: said storage element is further operable to contain a control indicator, said control indicator indicating that monitoring is only allowable for identified applications

(see combination used in claim 12); and said control logic is operable to check at least one identifier identifying an application that is allowable (Angelo col 7 line 61-64), said control logic only initiating said monitoring logic in the first domain when said application currently running is one identified as being one for which monitoring is allowable (Angelo col 7 line 61 to col 8 line 4)..

Regarding claim 32, Alverson/Angelo discloses the processor according to claim 31, said processor comprising a further storage element, said storage element being operable to contain said at least one identifier specifying an application that is allowable (Alverson col 1 lines 37-38).

Regarding claim 33, Alverson/Angelo discloses the processor according to claim 31, wherein said monitoring logic is operable to monitor the processor and capture diagnostic data (Angelo col 7 liens 61-64); and wherein said control logic is operable to control the monitoring logic to suppress capturing of diagnostic data in said first domain when said control logic detects that said application running is not one identified as being allowable (Alverson col 1 lines 37-38).

Note that if the processing system hasn't picked a particular application stream to run, then the monitoring of that application is considered to be suppressed.

Regarding claim 34, Alverson/Angelo discloses the processor according to claim 20, said processor further comprising an input port, wherein said control value is operable

to be set in said storage element either via the input port or via an input from said first domain (Angelo col 7 line 56-58).

Regarding claims 34-36, see claims 16-18, respectively.

Regarding claims 38 and 39, Alverson/Angelo disclose the use of a register holding the storage elements.

Note that according to the American Heritage College dictionary, a computer science definition of a register is "a part of a central processing unit used as a storage location."

Claims 9, 10, 17 and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alverson/Angelo in view of common art.

Regarding claim 9, Alverson/Angelo discloses the method according to claim 8, Alverson/Angelo discloses saving a portion of memory (Angelo col 7 lines 61-64).

Angelo fails to particularly disclose that the information includes instruction traces.

Examiner asserts that saving instruction traces is common in the art and can be utilized for many debugging purposes. Alverson/Angelo would have been motivated to utilize this technique to gather more debugging/security information for analysis. It would be further obvious to include a trace enable bit so the processor knows when to

save instruction traces.

Regarding claim 10, Alverson/Angelo discloses the method according to claim 9, wherein said secure domain enable value comprises a secure debug enable bit and a secure trace enable bit, initiation of debug and trace in said secure domain only being allowable if respective portions of said secure domain enable value are set (see claim 9).

Regarding claims 17 and 37, Alverson/Angelo discloses a method according to claim 16, wherein said first domain comprises a first user mode (Angelo col 1 lines 30-33) and a first privileged (Alverson col 2 lines 56-57) mode and said step of setting at least one control value in the first domain (Angelo col 8 lines 8-11),

Examiner asserts that it would have been obvious to require a non-privileged mode, domain, etc. to require an authentication code before accessing the control value of a privileged domain.

Examiner further asserts that Angelo/Alverson desired to have a form of security (Alverson col 2 lines 56-57 and Angelo col 8 line 4) and would be motivated to utilize this technique. Additionally, Angelo col 7 lines 15-24 shows the use of an authorization code, generally.

Response to Arguments

1. Applicant's arguments with respect to claims 1-39 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

2. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian P. Johnson whose telephone number is (571) 272-2678. The examiner can normally be reached on 8-4:30 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eddie Chan can be reached on (571) 272-4162. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EDDIE CHAN
SUPERVISO[illegible]ENT EXAMINER
TECHNO[illegible]2100